KAREN STEPHENS

Karen is CEO and co-founder of BCyber, an agile, innovative group that works with SMEs to protect and grow their businesses by demystifying the technical and helping them to identify and address cybersecurity and governance risks. In 2021 Karen graduated from the Tech Ready Woman Academy's Accelerator and the Cyber Leadership Institute's CLP programs.

COLUMN

A little knowledge of equality can help us all!

Equality comes in many shapes, sizes and forms. You have gender, cultural background, education and location, to name but a few. What unites them all? Regardless of type, is knowledge. The more you have, the better off you are, or to quote Sir Francis Bacon, "knowledge is power."

With 95 percent[1] of cybersecurity incidents the result of human error, imagine what could be done if we increased cybersecurity awareness across the "forgotten groups" of the population. If hardening our country's cybersecurity resilience is important, perhaps we should be doing more with groups that account for well over 50 percent of the population.

- **SMEs.** Why bother? Well, they are the backbone of the Australian economy, accounting for 99.8 percent of all enterprises and employing more than 7.6 million people[2]. Traditionally, SMEs have been left behind when it comes to cybersecurity. They are unable to afford the measures or staff available to big businesses. But they are the gatekeepers of the prime target of the cybercriminal: personally identifiable information[3]. To raise the profile of existing programs perhaps the SME associations could start profiling these in their conferences and discussion groups. Perhaps we in the cyber industry just need to let them know what is out there (in plain English and not "Tech Talk"!

- **School children.** Why bother? Australia has over four million enrolled[4] school students. If every school regardless of type or location had access to basic cybersecurity awareness programs imagine the difference it would make. If formal programs are beyond reach of a school's finances, what about volunteering your time to talk to the students. Why not go wild and include the staff and families. We need to arm our digital natives as much as we can and as soon as we can.

- **Retirees.** Why bother? There are more than 3.9 million[5] of them and they are generally the most vulnerable to cyber scams. Once again, it comes down to knowledge accessibility and availability. It is all very well for the government to provide "online assistance," but if you are not a digital native then you may not know which websites are trustworthy and which are not, or even know how to go about learning. Resorting to the old business adage of "it's not what you know, it's who you know," perhaps the fix is having cyber community members volunteer, for example by talking to retiree groups. This could also entail putting together formal (or informal) programs that government or relevant associations could rollout. However, these could require the cybersecurity community participants to committing time and money, luxuries some l retirees do not have. I do not know the answer, but I do know doing something is better than not doing anything at all.

Cybersecurity awareness should not be for the lucky few. Working together as an industry we can "spread the word" and we might just save a few more people from the cyber criminals.

SOURCES

(1) World Economic Forum finds that 95% of cybersecurity incidents occur due to human error | Cybernews
(2) 3. Australia | Financing SMEs and Entrepreneurs 2022 : An OECD Scoreboard | OECD iLibrary (oecd-ilibrary.org)
(3) What is personal information? | OAIC *(4)* Schools, 2022 | Australian Bureau of Statistics (abs.gov.au) *(5)* Retirement and Retirement Intentions, Australia, 2018-19 financial year | Australian Bureau of Statistics (abs.gov.au)

www.linkedin.com/in/karen-stephens-bcyber

www.bcyber.com.au *twitter.com/bcyber2*

karen@bcyber.com.au *youtube.bcyber.com.au/2mux*